PERFORMANCE ANALYSIS OF DIGITAL WATERMARKING OF IMAGE IN THE SPATIALDOMAIN

MS. L.R.GAJRIYA[1], PROF. MUKESH TIWARI[2], PROF. JAIKARAN SINGH[3], DR. ANUBHUTI KHARE[4]

[1]Department of electronics and communication engineering, SSSIST- Sehore, Rajiv Gandhi Proudyogiki Vishwavidhyalaya, University of M.P. (India)

[2]Associate Professor, Department of electronics and communication engineering, SSSIST- Sehore, Rajiv Gandhi Proudyogiki Vishwavidhyalaya, University of M.P. (India)

*3*Associate *Professor, Department of electronics and communication engineering, SSSIST- Sehore, Rajiv Gandhi Proudyogiki Vishwavidhyalaya, University of M.P. (India)*

4 Associate *Professor, Department of electronics and communication engineering, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidhyalaya, university of M.P. (India)*

ABSTRACT

In this paper, we have suggested the spatial domain method for the digital image watermarking for both visible and invisible watermarks. The methods are used for the copyright protection as well as proof of ownership. In this paper we have used spatial domain characteristics of the image where we directly work on the pixel value of the image according to the watermark and calculated differentparameters.

Keywords- Digital image watermarking, image copyright protection, special domain watermarking, Least Significant bit.

I. INTRODUCTION

In case of a dispute, identity was established by either printing the name or logo on the objects. But in the modern era where things have been patented or the rights are reserved (copyrighted), more modern techniques to establish the identity and leave it untampered have come into picture.

Unlike printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data.

A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in Figure 1 and 2 respectively

.

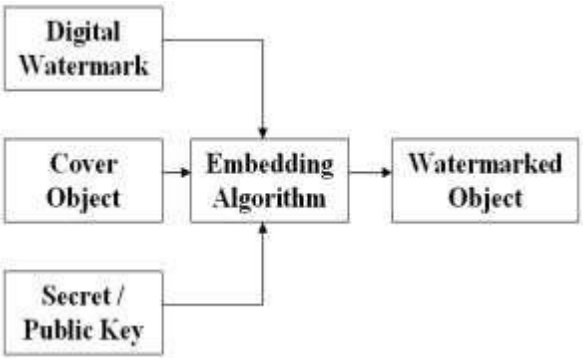

Fig. 1: Embedding process of watermarking

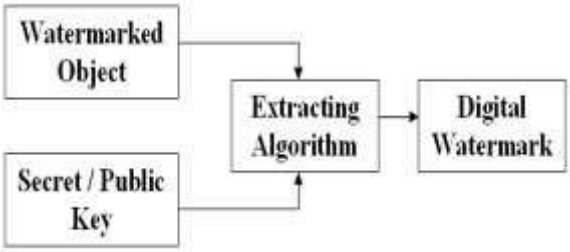

Fig. 2:Recovery process of watermarking

II. REQUIREMENTS OFWATERMARKING

A. Robustness

Robustness means that the watermarking scheme employed should be able to preserve the watermark under various attacks. The attack could be anything like rotation, translation, cropping, scaling or passing the image through various types of filters. There might be some noise introduced by this processing but this should not affect the retrieval of the watermark.

B. Imperceptibility

The imperceptibility refers to the perceptual transparency of the watermark. Watermarking should be done in a way such that it does not affect the quality of the image or the hidden data after watermarking. The changes in the image should not be noticeable to the naked eye. A straightforward way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host signal. However, this makes it easy for an attacker to alter the watermark information without being noticed.

C. Payload Capacity

Payload Capacity normally refers to the amount of information that can be embedded into a host signal. Various applications have different sizes of the data that is to be hidden. This directly affects the robustness and the perceptual impact. If too much of the data is hidden in the image

(much more than the payload capacity) it is harmful for the quality of image as the resolution of the images reduces drastically.

A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both which can be explained by Figure that shows the tradeoff between the Robustness, Imperceptibility and Payload Capacity.

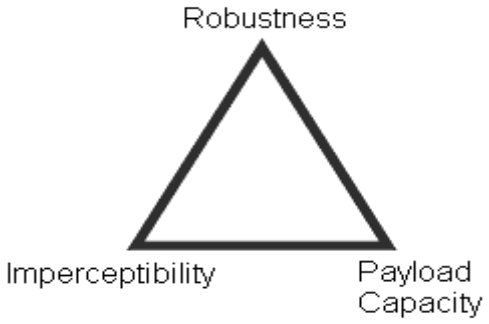

Fig.3:Tradeoff triangle

D. Reliability

There is always a possibility that the user knows the exact algorithm for detecting and rendering the watermark inactive. The only way to secure the watermark then lies in the selection of the key used for watermarking. Now, even if the user on the other side knows the exact algorithm it should be practically impossible to find the exact key to match with the one during embedding. This counts for the reliability or strength of the watermark.

III. THE SPATIAL DOMAINTECHNIQUES

Most of the early researches in digital watermark embedded the watermark in the spatial domain which is straightforward and less computationally expensive. Spatial domain watermarking involves slight modifications of image properties such as brightness, contrast or colour.

The method involves using the two-dimensional array of pixels in the container image to hold hidden data. In this point we discuss algorithm from the spatial domain to show how possible it is to embed binary text data and 2-D image in a digital image and discuss its applicability as visible as well as invisiblewatermarking.

A. VisibleWatermarking

Visible watermarking schemes are used to protect digital images that have to be released for some purposes, such as the contents used in learning websites or digital libraries, while illegal copying or reproduction is prohibited. A visible watermark is a secondary translucent overlay on the primary image and appears visible to a viewer on carefulinspection.

Visibly watermarked images often contain recognizable but unremarkable copyright patterns indicating the identity of intellectual property rights (IPR) owners. The main advantage of using visible watermarks is that it conveys an immediate claim of ownership. It also prevents or at least

discourages unauthorized use of copyrighted high quality images. A functional visible watermarking scheme should meet the following requirements:

(A) Perceptibility of host image details: all the details in the original host images should remain perceptible after watermarkembedding.
(B) Visibility of watermark patterns: the embedded watermark should be easily recognized from the watermarked images by the nakedeye.
(C) Adaptive spreading over host image: the visible watermark should be adaptively spread over a large or important area of host image to prevent its deletion byclipping.
(D) Robustness: embedded watermarks should be difficult or impossible to remove unless exhaustive and costly human interventions areinvolved.
(E) Efficiency: the watermark patterns should be applied automatically with little humanlabor.

1. EmbeddingAlgorithm

In the actual embedding algorithm we have gone through the following steps.

- When there is a black pixel (00000000) i.e non transperent part of the message, the corresponding pixel of the cover image is replaced with the black pixel so as to have a visualperception.
- When there is a white pixel (11111111) i.e transperent part of the message, the corresponding pixel of the cover image is kept as itis.

Fig.4:Embedding Process in visible watermarking Visible Watermarking

B. InvisibleWatermarking

1. Least Significant Bit SubstitutionMethod

The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object.

Consider an MxN image where M shows number of rows and N shows number of columns. In this image each pixel value is represented by a decimal number in the range determined by the number of bits used. In a gray-scale image, with 8 bit precision per pixel, each pixel assumes a value between [0, 255] and each positive number β10 can be represented by:

β10 = b0 + b1*G1 + b2*G2 + ……. where G = 2

This property allows the decomposition of an image into a collection of binary images by separating the bi into n bit planes. Figure 5 shows LSB decomposition of one Pixel.

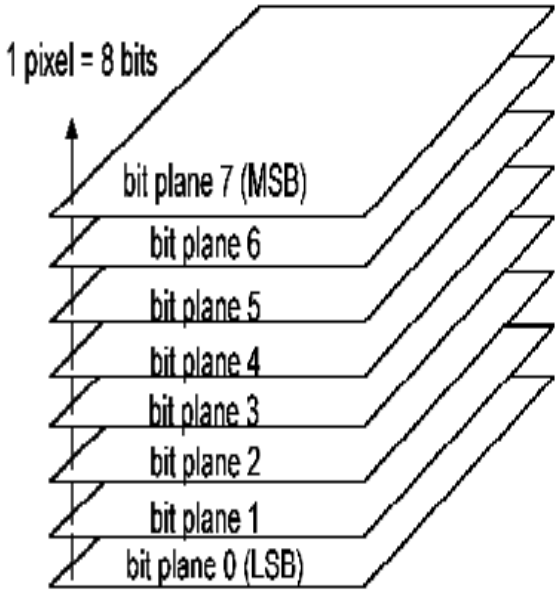

Fig.5:LSB decomposition of one pixel

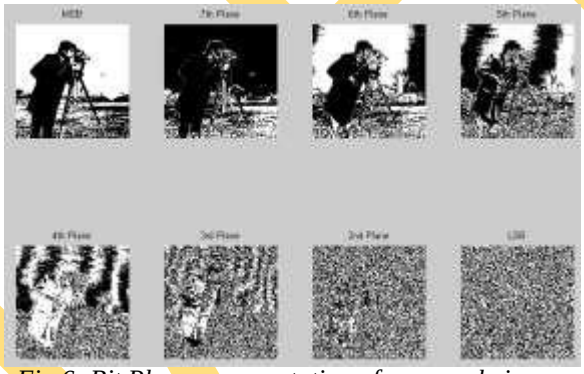

Fig.6: Bit Plane representation of gray scale image

Fig.7: Message image with only black & white Components with size 20x50

2. EmbeddingProcess

As it can be seen from the image that it has only two values [0 and 255] and its binary representations are 00000000 and 11111111 respectively. So here we can replace the MSB of the message image with the LSB of the Cover Image so that there is almost no visual degradation observed in the cover object.

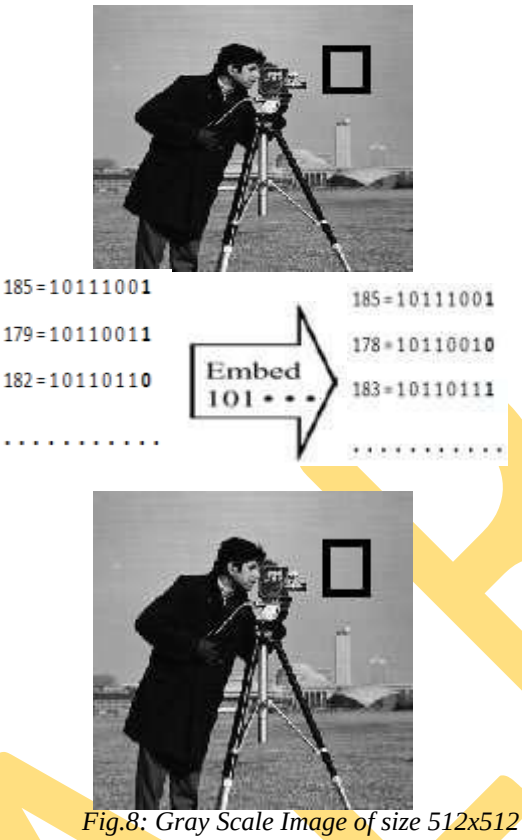

Fig.8: Gray Scale Image of size 512x512

LSB replacement Idea when message image is binary

Fig.9:Least Significant Bit is replaced with message

OriginalImage WatermarkedImage

Fig.10: Idea of Spatial Domain Watermarking Scheme

3. Extraction Process

For the watermark extraction, we can convert the watermarked image into its binary equivalent, extract the last bit and apply the following condition.

- If the extracted bit is 1, we would place a gray level of 255 in the respective place.
- If the extracted bit is 0, we would place a gray level of 0 in the respective place.

Figure 11 shows the Extracted message.

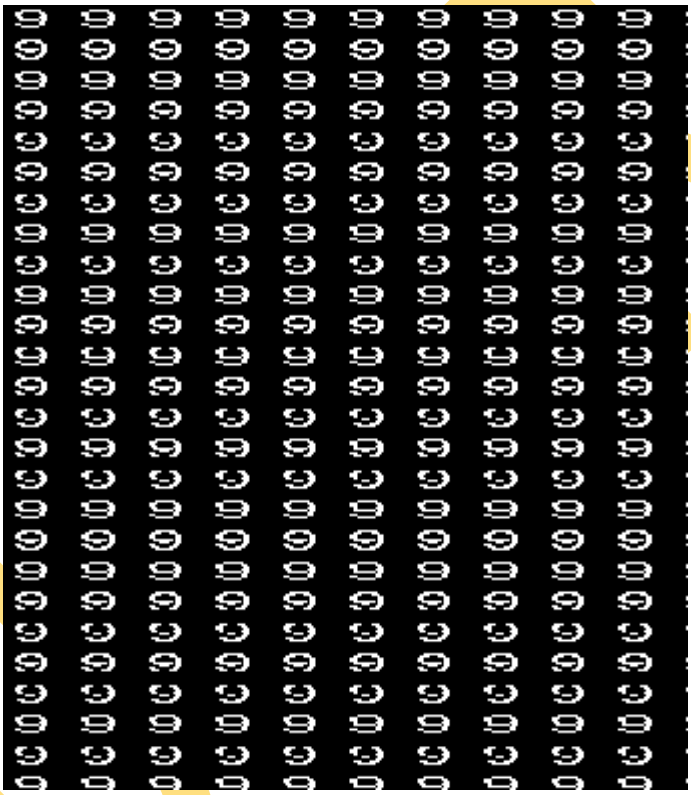

Fig.11: Extracted Watermark

Parameter	Value
Elapsed Time	**1.5022**
SNR	**46.7291**
PSNR	**51.1407**
MSE	**-3.0099**

Table 1. Table of Various Parameters measured with Spatial domain Technique

IV. CONCLUSION

The main advantage of such a technique is that the modification of the LSB plane does not affect the human perception of the overall image quality as the amplitude variation of the pixel values is bounded by ±1. The masking properties of the Human Visual System allow significant amounts of embedded information to be unnoticed or imperceptible by the average observer under normal viewingconditions.

V. REFERENCES

[1] M. A. Suhail and M. S. Obaidat, "Digital Watermarking-based DCT and jpeg Model" IEEE Trans. on Instrumentation and Measurement, vol. 52, no. 5, pp. 1640-1647, Oct.2003.

[2] J. R. Hernández, M. Amado, and F. Pérez-González, " DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", IEEE Tran. Image Processing, vol. 9, pp. 55-68, Jan.2000.

[3] Z. Lu,D. Xu, and S. Sun, " Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization" IEEE Trans Image Processing, vol. 14, no. 6, pp. 822 - 831, June2005.

[4] J-B. Zheng, D. D. Feng, and R-C. Zhao, "A Multi-Channel Framework for Image Watermarking", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August2005.

[5] P. Dong, et al., "Digital Watermarking Robust to Geometric Distortions", IEEETransactions on Image Processing, vol. 14, no. 12, Dec. 2005.

[6] W. Xing, Z. Lu, And H. Wang, "A Digital Watermarking Method Based on Classified Labeled-Bisecting-K-Means Clustering", Proceedings of The 2nd Inter. Conf. Machine Learning & Cybernetics, pp.2891-2895, Nov.2003.

[7] Q. Cheng, and T. S. Huang, "Robust Optimum Detection of Transform Domain Multiplicative Watermarks" IEEE Trans. Signal Processing, vol. 51, no. 4, pp. 906-924, April2003.

[8] F. Hartung, M. Kutter, "Multimedia watermarking techniques" Proceedings of the IEEE,vol. 87, issue 7, pp. 1079-1107, Jul 1999.

[9] D. P. Mukherjee, S. Maitra, and S. T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication" IEEE Transactions on Multimedia, vol. 6, no. 1, pp. 1-15, Feb.2004